VOMRS/VOMS-Admin Convergence

Andrea Ceccanti, Vincenzo Ciaschini, Maria Dimou, Gabriele Garzoglio, Tanya Levshina, Steve Traylen, Valerio Venturi

Open Science Grid

Fermilab

INFN Istituto Nazionale di Fisica Nucleare

eGee Enabling Grids for E-sciencE

Outline

- Virtual Organization Membership Service (VOMS)
- VOMS Registration tools
  - VOMS-Admin
  - VOMRS
- Joint Security Policy Group Requirements
- VOMRS-VOMS Admin convergence

Open Science Grid

Fermilab

INFN Istituto Nazionale di Fisica Nucleare

eGee Enabling Grids for E-sciencE

VO Membership Service

- Virtual Organization Membership Service
  - an Attribute Authority (AA) that issues attributes (in the form of signed assertions) expressing membership information of a subject in the context of a Virtual Organization (VO)
- VOMS extends X509 PKI AAI with VO specific information

- VOMS is a source of trust for authorization on the Grid so that access to Grid resources is regulated according to user's VOMS attributes
  - e.g, members of the Atlas VO can read this dataset/submit jobs at this CE etc...
- Grid users must be registered at a VO in order to obtain credentials that can be used to access Grid resources

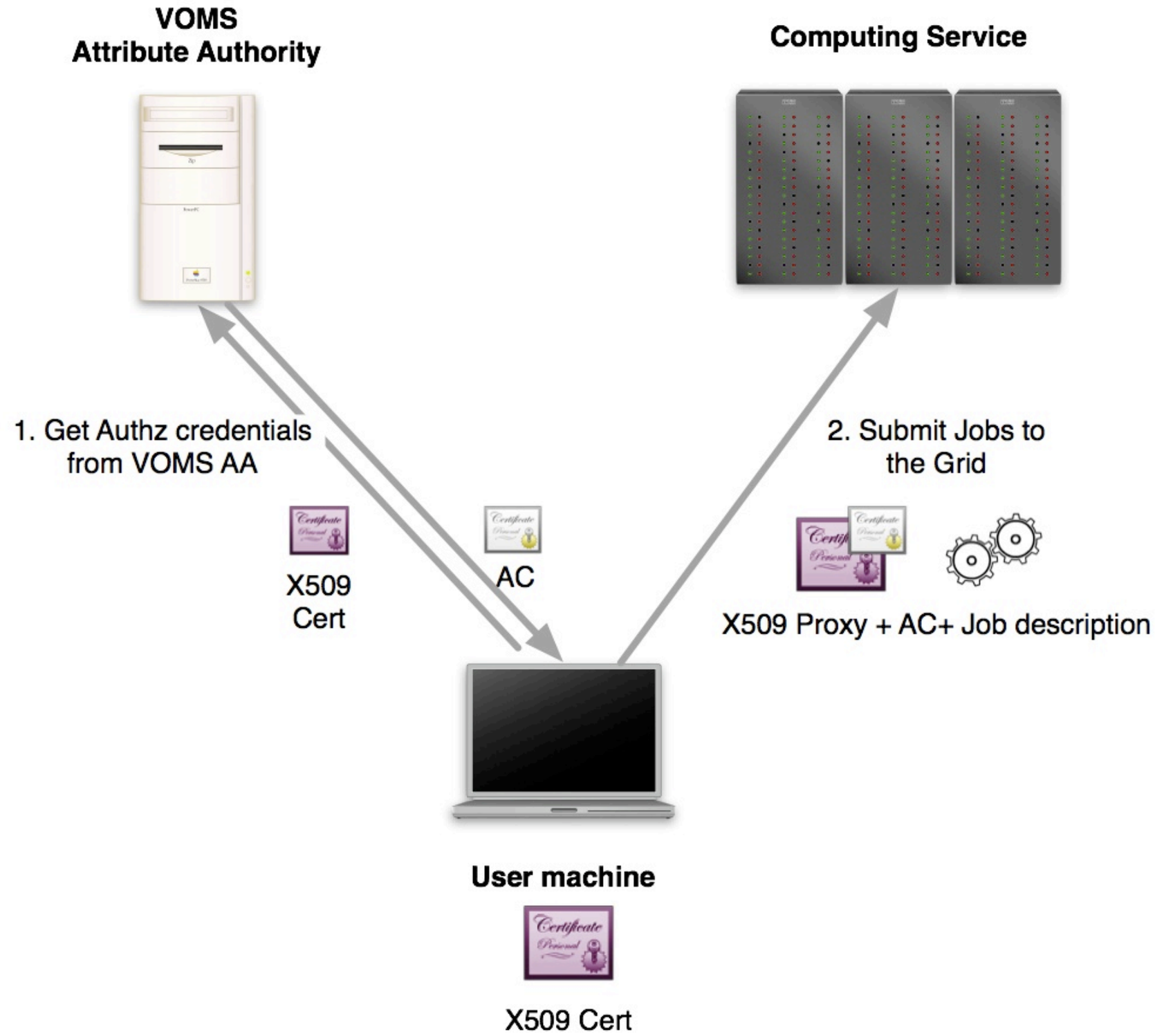
Open Science Grid

Fermilab

INFN Istituto Nazionale di Fisica Nucleare

eGee Enabling Grids for E-sciencE

VOMS Interaction



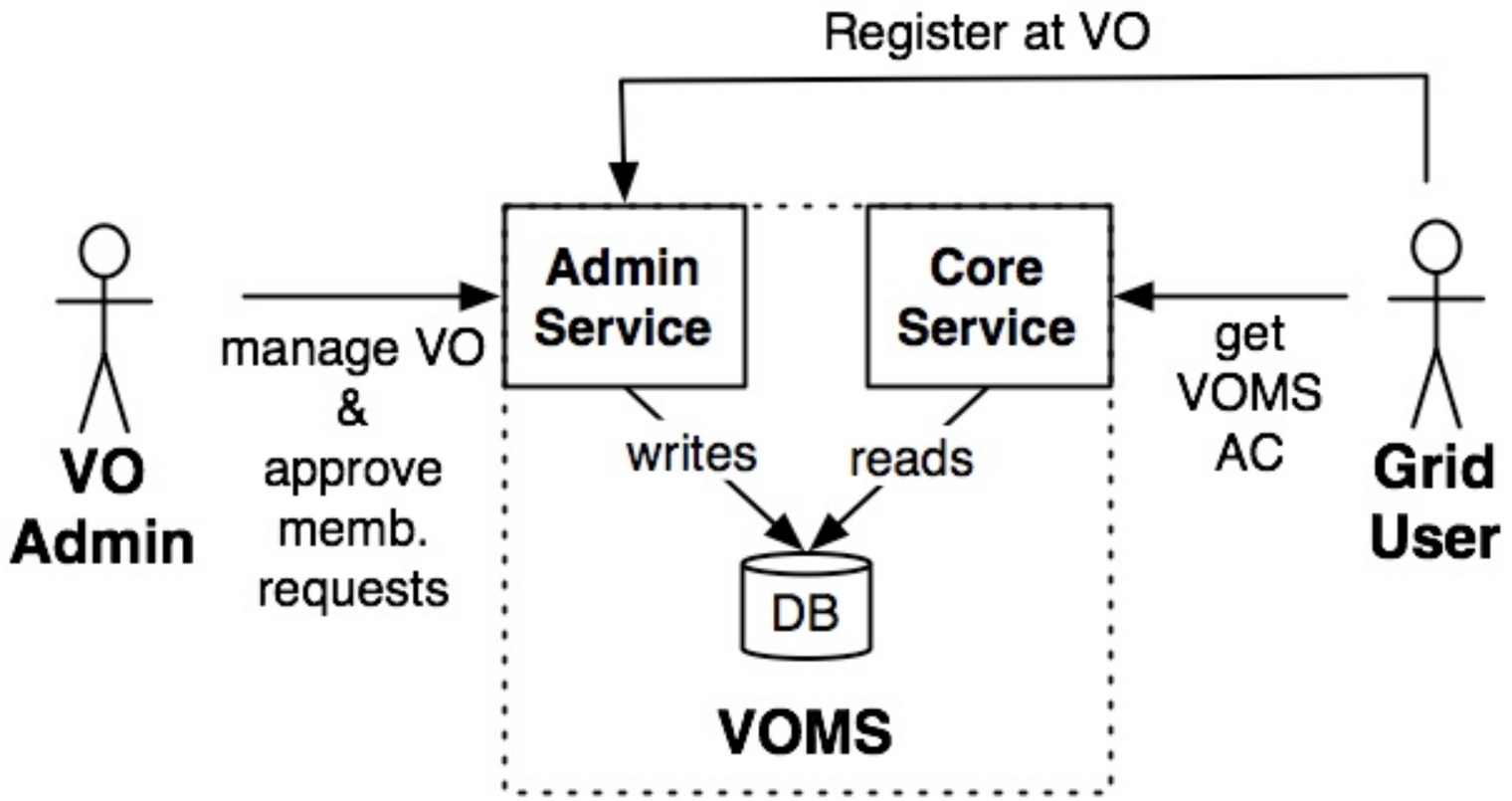
Open Science Grid

Fermilab

INFN Istituto Nazionale di Fisica Nucleare

eGee Enabling Grids for E-sciencE

VOMS services overview



- The **VOMS Admin** service is used to administer the VO structure and registration requests
- The **VOMS Core** service is contacted to obtain X509 attribute certificates (ACs) containing VOMS attributes by Grid users/ applications...

Open Science Grid Fermilab INFN Istituto Nazionale di Fisica Nucleare eGee Enabling Grids for E-sciencE

JSPG Requirements for VO registration

- The Joint Security Policy Group (JSPG) defined a set of requirements for VO membership Registration that must be implemented by all applications that manage user registration for WLCG Grid sites
  - http://www.jspg.org/wiki/Virtual_Organisation_Membership_Management_Policy
- A registration service that is compliant with JSPG rules supports:
  - Multiple administrative roles (VO Manager, Istitute Representative)
  - Collection of personal user data and management of multiple user certificates
  - Suspension/expiration/renewal of VO user's membership
  - Management and versioning of VO Acceptable Usage Policy (AUP)
  - Users requests for VOMS attributes assignment (Group, Roles, GAs)

Open Science Grid Fermilab INFN Istituto Nazionale di Fisica Nucleare eGee Enabling Grids for E-sciencE

VO registration services

- VOMS Admin
  - simple, streamlined registration (i.e., submit a request and wait for the admin approval)
  - **non** JSPG compliant
  - usually adopted by smaller VOs
- VOMRS
  - mature and flexible registration solution
  - JSPG compliant
  - well-suited to large VOs (LHC experiments)
  - works on top of VOMS-Admin and extends its registration functionalities

Open Science Grid Fermilab INFN Istituto Nazionale di Fisica Nucleare eGee Enabling Grids for E-sciencE

VOMS Admin in detail

- A J2EE Web application that
  - manages the contents of the VOMS database
  - provides a simple registration service
- Used by VO Administrators mainly to
  - add/remove users to the VO,
  - put them in VOMS groups,
  - assign VOMS roles to them
  - manage VOMS generic attributes
- Provides a Web Service interface to its functions
  - whose main clients are the VOMS Admin CLI and VOMRS

Open Science Grid

Fermilab

INFN Istituto Nazionale di Fisica Nucleare

eGee Enabling Grids for E-sciencE

VOMRS

- VOMRS was developed to address the end-to-end needs for VO membership registration and groupings of common interest within the WLCG and Fermilab contexts.
  - Initiated on 1/24/03, first production release - 3/1/2004.
- Some of the collected requirements were incorporated into JSPG VO Membership Management Policy document.
- The implementation is in compliance with JSPG requirements.
- VOMRS is part of OSG and the WLCG, and is available for EGEE VOs.

Open Science Grid

Fermilab

INFN Istituto Nazionale di Fisica Nucleare

eGee Enabling Grids for E-sciencE

VOMRS in detail

- Main features:
  - Sophisticated registration workflow and notification engine
  - multiple certificates per user management tools
  - interfaces to third-party systems to get/push relevant membership information
    - CERN and Fermilab HR databases, DZERO SAM, VOMS itself
- VO-level management of trusted Certification Authorities
- Sophisticated Group/Role management
  - Handles group/roles membership requests
  - Can associate a textual description to group/roles
  - Can link specific roles to specific groups
  - Can open/restrict access to a specific Group/Role

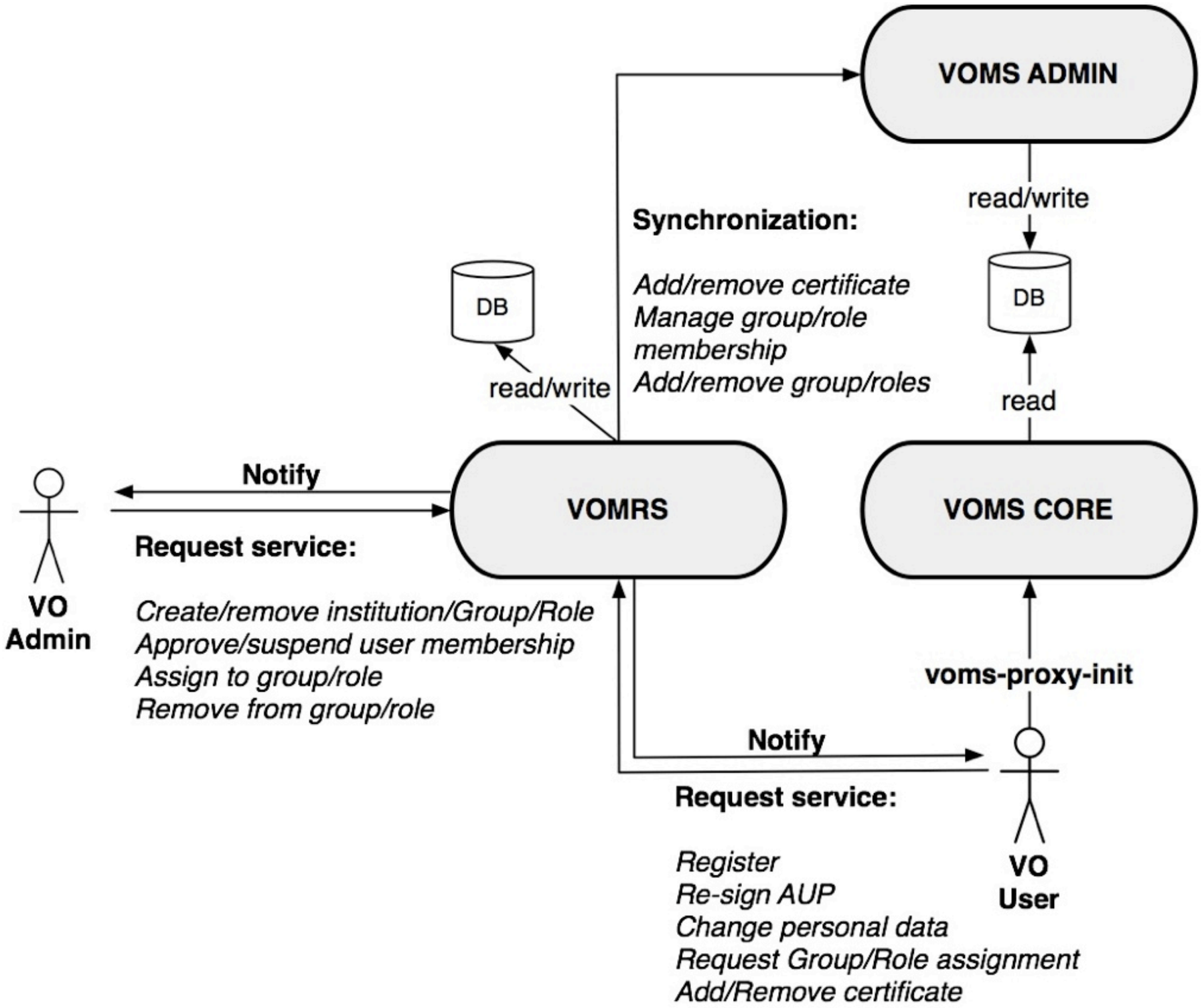
Open Science Grid

Fermilab

INFN Istituto Nazionale di Fisica Nucleare

eGee Enabling Grids for E-sciencE

VOMRS/VOMS-Admin Synchronization



Open Science Grid

Fermilab

INFN Istituto Nazionale di Fisica Nucleare

eGee Enabling Grids for E-sciencE

VOMRS/VOMS Admin convergence

- VOMS-Admin is emerging. This raises the possibility of rationalizing the support and converging on a single solution by continuing and extending our current collaboration.
- There is a keen interest in continuing our collaboration for several reasons. For example, as VOMS-Admin evolves, VOMRS/VOMS synchronization may necessitate VOMRS code changes and will require frequent testing.
- VOMS-Admin must become JSPG compliant anyway, so there will be a big feature overlap with VOMRS!
- Maintaining two almost equivalent VOMS registration services is not optimal in the long run and complicates deployment!

The Convergence Schedule

Phase I	Implement JSPG requirements	March 2009
Phase II	Migrate essential VOMRS features to VOMS Admin	Jan. 2010
Phase III	Interface with third party directory services (CERN HR db)	Spring 2010
Phase IV	Validation and certification tests	N/A
Phase V	Data migration from VOMRS to VOMS Admin	N/A

Open Science Grid

Fermilab

INFN Istituto Nazionale di Fisica Nucleare

eGee Enabling Grids for E-sciencE

Phase I

- To achieve JSPG requirements compliance, VOMS Admin is extended with:
  - collection of user personal information at registration time
  - multiple certificates support
  - VO membership suspension/expiration/renewal
  - AUP management support
  - VO member's ability to request group/role membership

- VOMS Admin 2.5 that implements these features is currently under testing and will be soon released to EGEE certification.

Open Science Grid Fermilab INFN Istituto Nazionale di Fisica Nucleare eGee Enabling Grids for E-sciencE

Phase II

- Migration of essential VOMRS features:
  - More flexible management of member's status and list of collected personal information
  - Enhanced handling of VO groups and roles
  - Interfacing third-party directory services during registration and membership validation
  - More flexible registration workflow and event notification
  - Web UI improvements (sortable output, operations on multiple users, online help)
- ETA: early 2010

Open Science Grid Fermilab INFN Istituto Nazionale di Fisica Nucleare eGee Enabling Grids for E-sciencE

Phase III

- Interface with third party directory services:
  - A generic framework to plug external services at member registration or validation is implemented in VOMS Admin
  - A CERN HR database plugin is developed and becomes part of the standard VOMS Admin distribution
  - The framework is general enough so that other teams may develop their external directory service plugin easily!
    - DZERO plugin developed at Fermilab

Open Science Grid

Fermilab

INFN Istituto Nazionale di Fisica Nucleare

eGee Enabling Grids for E-sciencE

Phase IV & V

- Validation and certification testing is done on the new codebase to ensure
  - Migration of all needed functionality
  - Robustness and scalability
  - Backward compatibility with existing services and clients

- It is not yet clear how this effort will be fundegd
  - gLite consortium, EGI, IGI?

Open Science Grid

Fermilab

INFN Istituto Nazionale di Fisica Nucleare

eGee Enabling Grids for E-sciencE

Summary

- VOMRS and VOMS were developed to address the end-to-end needs for VO membership registration and groupings of common interest within the WLCG and Fermilab contexts.
- VOMRS has crucial features that has been proven to be essential for registration of big VOs
- Fermilab is committed to the support and maintenance of VOMRS in the short and longer term.
- The recent development of new features in VOMS-Admin raises the possibility of rationalizing the support and converging on a single solution by continuing and extending our current collaborations, however it is not yet clear how the last phases of this convergence plan will be funded

Open Science Grid Fermilab INFN Istituto Nazionale di Fisica Nucleare eGee Enabling Grids for E-sciencE